SECURE ONLINE PAYMENT SYSTEM AND ONLINE PAYMENT AUTHENTICATION METHOD

Field of the Invention

[1] The invention relates to a secure online payment authentication method and a secure online payment system that utilizes said method.

Background of the Invention

[2] In recent years, e-business has become the main trend in development of Internet-based economy, and online shopping payment has become a convenient life style gradually. A key link in e-business is the payment settlement system, and online payment is the ideal payment solution for e-business.

[3] At present, major online payment means include bank card, electronic check, and electronic wallet, etc.; wherein, bank card is the most widely used payment means.

[4] The online payment system disclosed in the invention mainly involves bank account-based payment means (e.g., bank card) and a payment method that accomplishes e-business transactions over Internet.

[5] The key challenge in online payment is security.

[6] E-business must be undertaken in a secure environment, which involves three implications:

[7] 1. Data security

[8] The online transaction data must not be intercepted and stolen and there by embezzled illegally in the transmission process.

[9] 2. Data integrity

[10] The online transaction data must not be modified, lost so as to be distorted in the transmission process.

[11] 3. Authenticity of subjects

[12] Online transactions must be made on condition that the consumer involved in the transaction is right the legal card holder or the owner of the bank account, and the vendor is a legal merchant.

[13] Online payment faces the following challenges:

[14] Security and integrity of transaction data

[15] The transaction data is transferred over Internet, which is an open network; therefore, the transaction data may be intercepted, stolen, or tampered, and thereby used illegally.

[16] Authentication of subjects of transaction

[17] In the traditional online payment process, the card holder is usually not authenticated, and the consumer can complete a transaction successfully merely by entering the credit card ID and the expiration date; since both the card ID and the expiration date are not confidential, they can be embezzled easily. As the result, it is inevitable there are more and more online payment fraud cases.

[18] In order to solve the above problems, diverse security authentication means are invented, mainly including the following technical means:

[19] Secure Socket Layer (SSL) encryption mechanism

[20] SSL is an encryption algorithm. It is a secure data transmission protocol over network issued originally by Netscape, with the main purpose to provide a secret and reliable connection between the two parties involved in communication. SSL handshake protocol enables the server and the customer to authenticate each other with a specific encryption algorithm before data transmission. The advantage of SSL lies in: it is an independent application protocol, on which higher levels of protocols can be established.

[21] Most Web Servers and Browsers support SSL-based encrypted data transmission. Therefore, with this feature, partial web pages of

confidential nature can be set in encrypted transmission mode, so as to prevent the data from being intercepted by any third party when the data is transmitted over the network. SSL utilizes a public key encryption technique (RSA) as the protocol for encrypted data communication between the customer and the server. Presently, most Web Servers and Browsers use SSL technology. For consumers, SSL has solved most of the problems. However, for e-business, the problems are not solved completely, because SSL can only ensure data security, but the vendor can't determine the actual provider of the data; even though the data provider can be ascertained, there is still a problem regarding settlement with the bank.

[22] Secure Electronic Transaction (SET) specification

[23] In 1996, SET is developed by MasterCard International, Visa International, and American Express International, together with IBM. SET is a perfect technical product, and specifies authentication with digital certificate for the card holder, merchant, and bank. SET utilizes RSA secure public key encryption technique, featured with data security, integrity, and identifiability and non-repudiation of data source. It provides the standard for protecting consumers in payment for online transactions with credit card over Internet.

[24] SET involves Electronic Wallet, Merchant Server, Payment Gateway, and Certification Authority (CA), which constitute SET-compliant authorized transactions with credit card over Internet.

[25] SET is used from the commercial site to the commercial bank through the browser at the customer in secure online payment system with electronic bank card. The online bank uses existing programs and equipments to identify the credit card and settle the consumer's bank account, so as to complete the transaction. SET ensures security of the entire payment process by concealing the credit card ID. To

this end, SET must ensure the credit card holder is connected persistently to the bank in the existing system over the network. SET creates a complete solution for using credit cards in different systems. Due to its reliable identity authentication, SET is an excellent online payment system. It ensures each legal participant in the transaction possesses a legal identity and the identity verification for the card holder is performed by the bank. Of course, there are other services involved, such as identity authentication and customer service, etc. It is the method of establish another reliable customer connection. In addition, it can facilitate arbitration in case of any dispute.

[26] To authenticate with the certificate, the certificate software must be installed on the computer of the object to be authenticated; such an approach is viable to authenticate the merchant; however, that approach will bring inconvenience when it is used to authenticate the card holder, because many online shoppers may not always use a fixed computer to access Internet.

[27] Therefore, the solution has the following drawbacks:

[28] (1) Under SET protocol standard, the merchants around the world have to be certified in certification authorities, and the consumers have to obtain electronic certificates from the certification authorities, which brings severe inconvenience to the consumers.

[29] (2) Under SET protocol standard, the merchants have to install complex software on their servers, and the consumers have to install complex software on the PCs, in order to make e-business transactions and store electronic certificates; as the result, the consumers will be frustrated.

[30] (3) Due to the fact that the electronic certificate of a consumer has to be installed on a fixed PC, the card holder's

e-business transactions have to be made through that PC, which causes severe limitations to the e-business.

[31] (4) Since the electronic certificate has to be installed on the consumer's network access device, it is impossible to make e-business transactions with network access devices on which an electronic certificate can't be installed, such as mobile telephones and PDAs, etc.

[32] (5) In micro-transactions, the consumer's cost for the transaction is even higher than the value of the transaction; therefore, the consumer has no impetus to use SET protocol in micro-transactions.

[33] 3D SET standard

[34] 3D SET standard is put forth on the basis of SET, with the following improvement:

[35] 1) Under 3D SET, the consumer is not required to install complex software on his/her PC (or any other Internet access device) to make e-business transactions and store electronic certificate.

[36] 2) In a 3D SET environment, the consumer can make e-business transactions and obtain certification from the card issuer through any network access device instead of merely through a PC, since the consumer is not required to store electronic certificate on a PC.

[37] However, the 3D SET standard still has the following defects:

[38] 1) Similar to other certificate-based authentication methods, it requires the consumer to possess electronic certificates from card issuing authorities for all his/her bank cards. Since a consumer usually possesses more than one bank cards on hand, it is troublesome for the consumer to obtain electronic certificates from corresponding card issuing authorities for all these cards.

[39] 2) Since the consumer can make e-business transactions through any network access device, certificate-based authentication

is unnecessary and troublesome when compared to password-based authentication.

[40] 3) 3D SET is not compatible to SSL. Due to the fact that SSL is well recognized and widely used in data transmission for online payment in actual e-business, SSL often is the de-facto standard for e-business; therefore, it is difficult to generalize the application of 3D SET.

[41] Visa 3D Secure system

[42] In 2001, the Visa international credit organization put forth Visa 3D Secure system.

[43] Visa's 3D is not merely a payment and authentication method or a technical scheme; virtually, Visa 3D Secure is a complete secure online payment authentication system. In this payment authentication system, it is required to authenticate the card holder (by the card issuer) and the merchant (by the acquirer).

[44] The word "3D" in 3D Secure is the abbreviation of "3 Domains", i.e., three domains. The three domains are: Issuer Domain (including the card holders and the card issuers), Acquirer Domain (including the merchants and their acquiring entity), and Interoperability Domain (Visa).

[45] The obvious advantages are:

[46] 1) It minimizes the requirement for hardware/software of the card holder participating in e-business. The card holder is only required to have a computer installed with a browser (for example, IE) to access the network.

[47] 2) Compared to SET standard, Visa 3D Secure system only requires the merchant to authenticate the card holder but doesn't require the card holder to authenticate the merchant. The identity of the merchant is authenticated by a CA that is certified by Visa with the certificate.

[48] 3) It substitutes certificate-based authentication with password-based authentication, and thereby significantly simplifies the authentication procedures.

[49] The drawbacks include:

[50] Since 3D Secure system employs an "authentication + CA" network architecture, several procedures has to be added in each transaction process; therefore, the transaction process will spend more time.

[51] The card holder has to fill all detailed transaction information; when the card holder makes transactions at multiple merchants, the card holder has to enter password for each transaction.

[52] In this authentication scheme, the card issuer has to install complex server to support online transactions, so as to provide registration and authentication services for card holders.

[53] Visa 3D Secure system employs a centralized network architecture, and all authenticators require intervention of Visa Directory; viewed from the aspect of transaction flow, Visa Directory is not an efficient technical scheme: it delays the information flow and requires additional information transfer procedures, and thereby finally affect the entire transaction flow, and is subject to attacks from hackers; the authentication mechanism also employs a SSL encrypted data transmission protocol. Due to the fact that the card holder authorization process is separated from the certification process, fraudulent merchants can control MPI easily to obtain card holder information illegally, viewed from the authentication process. To prevent about fraud, 3D Secure requires the merchant to obtain a digital certificate from a CA that is certified by Visa, which, of course, enhances security of the 3D Secure system, but causes increased complexity in operation of the 3D Secure system.

[54] In conclusion, the defects in traditional or existing online

payment security systems include:

[55] SSL

[56] Though SSL implements point-to-point secure data transmission and ensures integrity and security of data transmission, SSL doesn't support authentication of the subjects involved in transactions and provide no means to authenticate legality of identities of the subjects; therefore, online payment can not be secured merely with SSL.

[57] However, SSL is a matured technology in itself and has been widely used. All other technologies that occurred subsequently, including SET, 3D SET, and the latest 3D Secure system, embed SSL encryption technology in their kernels.

[58] SET

[59] The worst defect in SET lies in the severe dependence to certificate-based authentication, mainly the certificate-based authentication method for card holders. Since the card holders are highly distributed, mobile, and numerous, though the card holders can be fixed and authenticated in e-business by means of issuing certificates to card holders, it is impracticable in practice.

[60] 3D SET

[61] 3D SET is a defective authentication system essentially because it inherits the defect of certificate-based authentication for card holders in SET; in addition, another apparent defect in 3D SET system is the incompatibility to SSL.

[62] 3D Secure

[63] 3D Secure has a blind spot behind its ostensible perfection, i.e., the password-based authentication mechanism will fail in case the card ID and the password are embezzled illegally. In addition, the card holder, merchant, card issuer, and acquirer have to carry out technical renovation and upgrade in part or in all, in order to

support normal operation of the authentication system.

Summary of the Invention

[64] The invention aims to provide a secure online payment authentication method and a secure online payment system, which are secure enough to prevent the customer's important information (banking information, e.g., credit card ID) from being intercepted by other people in the network as well as have high processing efficiency and require low cost; in addition, the authentication method is convenient and especially provides a convenient experience to the customer and the merchant in transaction activities.

[65] Through analysis of above existing techniques, we can conclude:

[66] SSL encrypted data transmission protocol is a proven technique and still can be utilized;

[67] The certificate-based authentication scheme for card holders is perfect theoretically but has a poor feasibility in practice;

[68] Substituting transparent data transmission with encrypted data transmission is an effective security measure, and the tractions will be more secure if the information of card holder can be isolated from the merchant and the acquirer;

[69] The merchant, the acquirer, and the card issuer shall be authenticated with certificates objectively and appropriately.

[70] The present invention provides a secure online payment authentication method and a secure online payment system with the following technical schemes:

[71] An online payment system in an aspect of the present invention, including:

[72] customer, i.e., the buyer, which is the party that a certain amount of money will be deducted from his/her account to pay a

merchant;

[73] the customer's bank of account or agency bank, i.e., the party that can confirm the customer's account information and execute deduction for payment;

[74] merchant, i.e., the service provider or merchandise provider, which is the party that will collect the payment;

[75] the merchant's bank of collecting account or agency bank, which is the party that can confirm the merchant's account information and receive payment from the customer, also referred to as the payee's bank of account;

[76] a payment gateway, which is a system responsible for handling payment information from the network, authenticating the customer and the merchant, and confirming authenticity and validity of a transaction;

[77] the customer, the merchant, and the payment gateway being connected to each other over Internet; after the processing system of the payment gateway confirms legality of the transaction, the payment gateway sending a payment request, and, after the payment is completed, informing the two parties (i.e., customer and merchant) involved in the transaction of the payment information;

[78] the payment gateway communicating with the customer and the merchant at one side to authenticate identity of the customer and identity of the merchant (password-based identity authentication for the customer, and certificate-based identity authentication for the merchant) and confirming the transaction and transaction value; and the payment gateway communicating with the bank of paying account and the bank of collecting account at the other side, to transfer payment request and deduction information;

[79] in order to ensure security of transaction and prevent the transaction information and relevant identity information and bank's

information from intercepted illegally over the network, an assistant customer identity authentication system is provided between the payment gateway and the customer; said assistant authentication system connects the customer to the payment gateway through a non-Internet approach; after the payment gateway confirms the customer's identity preliminarily with password and receives the payment request over Internet, it generates an authorization code and sends the authorization code to the customer via the assistant customer identity authentication system; after the customer receives the authorization code, the customer enters the authorization code on the correct page in the payment gateway; after the payment gateway verifies the authorization code, the payment gateway confirms the customer identity, sends the payment information to the bank, obtains the processing information from the bank, and forwards the processing information to the customer and the merchant.

[80] Said assistant customer identity authentication system includes a customer terminal and an switch system; said customer terminal has its initial information registered in the payment gateway; said switch system connects said customer terminal to said payment gateway, and receives information from said payment gateway and forwards the information to said customer terminal.

[81] Said switch system is available in different types, and the specific type is chosen by the payment gateway in accordance with said customer terminal. The information received by said switch system from said payment gateway includes authorization code and transaction information.

[82] Said authorization code is generated dynamically and has a validity period; it is deemed as valid only when it is inputted on the correct page in the payment gateway within the validity period; otherwise it will be deemed as invalid.

[83] Said customer terminal of the assistant customer identity authentication system is a dedicated device, and has its initial information registered in the payment gateway.

[84] Said customer terminal can be a dedicated device separately configured and provided by the payment gateway provided that it conforms to the standard of the payment gateway; or, said customer terminal can be a dedicated card provided by the payment gateway and inserted in a personal or home electronic or electrical device, such as a STB or a remote controller.

[85] Of course, the customer terminal of said assistant customer identity authentication system can be a non-dedicated device, such as a telephone, a mobile telephone, a BP, or a PDA, etc.; before said non-dedicated device is used as the customer terminal, it shall have its initial information registered in the payment gateway or a place designated by the payment gateway.

[86] The initial information of said customer terminal registered in the payment gateway may be one or more information of the customer terminal. Said customer terminal that is used to receive the authorization code may not be a customer terminal with initial information registered in the payment gateway.

[87] In the online payment system, there is arranged a bank's information processing system between the payment gateway and the bank; said bank's information processing system is connected to the payment gateway, the payer's bank of account, and the payee's bank of account; the payment gateway sends the payment request to said bank's information processing system to verify the payer's account can be used in the payment, obtains the processing result (successful deduction or payment rejection) of the payment request from the system.

[88] Said payment gateway and said bank's information processing

system can be network platforms provided by the same entity or different entities.

[89] Said bank's information processing system can be a network platform provided by the payer's bank of account or a network platform provided by the payee's bank of account or agency bank.

[90] Said payment gateway and said bank's information processing system can be network platforms provided by a third party irrelevant to the transactions.

[91] In another aspect of the present invention, there is provided an online payment authentication method that employs the online payment system provided in the invention, includes authenticating the two parties (i.e., the customer and the merchant) involved in the online transaction, and verifying the transaction and transaction value; wherein dynamic assistant identity authentication for the customer is also performed, besides the certificate-based identity authentication for the merchant and the password-based identity authentication for the customer.

[92] After the customer browses the web pages provided by the merchant and submits a transaction request and the merchant receives that transaction request, the online payment authentication method provided in the invention will begin. Specifically, said method includes the following steps:

[93] the customer initiating a payment request on a web page provided by the merchant and entering into the interface of the payment gateway;

[94] the payment gateway requesting the customer to enter his/her online PIN and password for online payment over Internet for customer identity authentication and verifying said password;

[95] when the password for online payment is incorrect, the payment gateway rejecting the payment request; when the password for online

payment is correct, the payment gateway generating an authorization code dynamically and going to the next procedure;

[96] the payment gateway sending the authorization code to the customer via the assistant customer identity authentication system;

[97] the customer entering the authorization code on the correct page in the payment gateway after he/she receives the authorization code;

[98] the payment gateway confirming the customer identity has passed the authentication after it verifies the authorization code successfully and then sending a payment request.

[99] In the above steps, said assistant customer identity authentication system forwards the authorization code to the customers is performed through a non-Internet approach.

[100] when a mobile telephone is chose as the customer terminal and a SMS is chose as the switch system for the assistant authentication system, the online payment authentication method in another aspect of the present invention includes the following steps:

[101] the customer sending a payment request on a web page provided by the merchant and entering into the interface of the payment gateway of the online payment system, choosing SMS-based authentication as the assistant identity authentication mode , and entering the mobile telephone number and the specified password for online payment at the prompt on the interface;

[102] when receiving the customer information, the payment gateway judging the mobile telephone number and the password for online payment; if said mobile telephone number has initial information registered in the payment gateway and the password is correct, the payment gateway generating a authorization code dynamically;

[103] the payment gateway sending said authorization code and the customer's mobile telephone number to the SMS center;

[104] the SMS center sending the received authorization code to the customer's mobile telephone;

[105] when receiving the short message, the customer entering the authorization code on the payment page at the prompt on the page;

[106] after verifying the authorization code successfully, the payment gateway deeming the customer's identity has passed the authentication and executing the subsequent payment procedures.

[107] The authorization code is generated dynamically, with a validity period; it must be inputted within the specified validity period.

[108] The payment gateway sends said authorization code to the customer (i.e., the customer terminal) via the assistant customer identity authentication system; said customer terminal can be a customer terminal with initial information registered in the payment gateway or a customer terminal chosen or specified by the customer.

[109] The information received by said switch system from said payment gateway includes authorization code and transaction information. Likewise, the information sent to the customer can include authorization code and transaction information.

[110] The switch system can use existing facilities, such as telecom networks and CATV networks, etc.

[111] The customer terminal of said assistant customer identity authentication system can be a dedicated device separately configured or configured in any other electronic or electrical device such as a STB or a remote controller; or, the customer terminal of said assistant customer identity authentication system can be a non-dedicated device, such as a telephone, a mobile telephone, or a PDA; however, before the non-dedicated device is used as the customer terminal, it shall have its initial information registered in the payment gateway or a place designated by the payment gateway.

Detailed Description of the Embodiments

[112] In order to describe the invention better, the following terms or phrases used in the online payment system according to the embodiments of the present invention are defined first:

[113] Customer - buyer, i.e., the purchasing party in e-business, the bank card holder, and the online payment initiating party.

[114] Payment gateway - it is an information transform system between Internet and the internal transaction processing system of bank (i.e., bank's information processing system), mainly responsible for processing payment information from Internet. It may be a public platform or a dedicated platform provided by an switch system, or a platform provided by a bank, or a platform provided by an agent bank.

[115] Card issuing bank - the card issuing bank performs verification and financial processing for the bank card payment information from the customer via the payment gateway and returns the processing result. It includes the payee's bank of account or the payer's bank of account. Narrowly spoken, it is the bank card-issuing bank; broadly spoken, it can be any form of bank of account.

[116] Online merchant - an e-business enterprise that provides merchandise or services and receive payment in the form of bank card over Internet; the online merchant can be directly connected to the payment gateway of the card issuer, or connected to the gateway of the card issuer via a payment agency.

[117] Payment agency - a professional entity that provides payment collection service over Internet to online merchants. If the card issuing banks maintain their payment gateways respectively, the payment agency can be connected to the payment gateways of multiple or even all card issuing banks to support payment with different bank

cards and settle with the card issuing banks on behalf of the merchants; if there is no such a payment agency, a merchant has to connect to multiple card issuing banks to support payment with different bank cards; if the payment gateway is provided by a third party and is connected to bank's information processing systems of multiple or all card issuing banks, the payment agency takes the same role as the payment gateway. In this invention, the role of the payee's bank of account or the payer's bank of account can be substituted by the payment agency.

[118] Bank of settlement of online merchant - the bank of account of online merchant, which provides financial settlement service to the merchant.

[119] Certification Authority (CA) - CA is an authority established to verify identity and standing of the parties involved in e-business transactions, to protect transaction security, and to provide essential guarantee for normal operation of e-business transaction activities.

[120] Online payment mainly involves the following links:

[121] The customer submits an order to an online merchant over the network; after the payment is confirmed, the customer and the online merchant enter into the online payment process, which mainly includes 4 links:

[122] Customer authentication - due to the fact that most online payments are transactions without card or magnetic strip, how to solve the customer identity authentication problem is an important link in online payments.

[123] Order confirmation - it is a required link for online payment, involving merchant authentication.

[124] Withdraw (or authorized deduction) by the card issuer - after the customer and the order are confirmed, the card issuer can perform

withdraw (or authorized deduction) from the customer's account. The completion of withdraw (or authorized deduction) by the card issuer indicates successful online payment; then, the merchant can provide the specified merchandise or service to the customer.

[125] Settlement with merchant - the bank of settlement of the merchant transfer fund to the merchant.

[126] Hereunder the system composition according to embodiments of the invention is detailed.

[127] An online payment system, including:

[128] customer, i.e., the buyer, which is the party that a certain amount of money will be deducted from his/her account;

[129] the customer's bank of account or agency bank, which is the party that can confirm the customer's account information and deduct money from the customer's account, also referred to as the payer's bank of account;

[130] merchant, i.e., the service provider or merchandise provider, which is the party that will collect the payment;

[131] the merchant's bank of collecting account or agency bank, which is the party that can confirm the merchant's account information and receive payment from the customer, also referred to as the payee's bank of account;

[132] payment gateway, which is a system responsible for handling payment information from the network, authenticating the customer and the merchant, and confirming authenticity and validity of the transactions;

[133] the customer, the merchant, and the payment gateway are connected to each other over Internet; after the processing system of the payment gateway confirms legality of the transaction, the payment gateway sends a payment request, and, after the payment is completed, informs the two parties (i.e., customer and merchant)

involved in the transaction payment of the payment information;

[134] the payment gateway communicates with the customer and the merchant at one side to authenticate identity of the customer and identity of the merchant (password-based identity authentication for the customer, certificate-based identity authentication for the merchant), and confirms the transaction and transaction value; the payment gateway communicates with the bank of paying account and the bank of collecting account at the other side, to transfer payment request and deduction information;

[135] In order to ensure security of transaction and prevent the transaction information and relevant identity information and bank's information from intercepted illegally over the network, an assistant customer identity authentication system is provided between the payment gateway and the customer; said assistant authentication system connects the customer to the payment gateway through a non-Internet approach. Said assistant customer identity authentication system includes a customer terminal and an switch system; said customer terminal has its initial information registered in the payment gateway; said switch system connects the customer terminal to the payment gateway, and receives information from the payment gateway and forwards the information to the customer terminal.

[136] Before the customer can make online transactions, the customer has to have his/her initial information registered in the payment gateway, i.e., the mapping information between customer identity and customer account as well as the basic information of the customer have to be registered; the payment gateway has other information stored in database or in other recording means, for example, the mapping information between customer account and the customer's bank of account, etc.; the customer can make online transactions with

his/her actual identity or the identity for online transaction (i.e., online PIN) mapped to his/her actual identity. Before the payment gateway handles the transaction request, it verifies whether the customer's identity provided over the network has been registered in it; if the customer's identity provided over the network is correct, the payment gateway will deem that the customer has passed the preliminary customer authentication and permits the online transaction. In addition, the payment gateway can request the customer to enter the password for online payment as specified in the registration of initial information after it verifies the customer's identity, so as to confirm the customer's identity has passed the preliminary authentication. The customer can provide a password for online payment for a dedicated customer terminal through the dedicated customer terminal (i.e., the payment gateway or an entity certified by the payment gateway), or specify a password for online payment when the customer makes an initial information registration at a place designated by the payment gateway. Said password can be modified by the customer.

[137] After the customer registers the initial information in the payment gateway, he/she can begin to make online transactions conveniently and securely. If the customer has specified a password for online payment, he/she can use the password for preliminary identity authentication at the time of customer identity authentication. In this way, the entering of bank card ID or any other account ID or corresponding password on the interface over Internet can be avoided during online transactions. That means the customer's actual identity is "shielded" and the customer's actual bank data is protected.

[138] After the payment gateway authenticates the customer's identity preliminarily with the password and receives the payment

request over Internet, it generates an authorization code, and sends the authorization code to the customer via the assistant customer identity authentication system; after the customer receives that authorization code, the customer can enter the authorization code on the correct page in the payment gateway; after verifying the authorization code successfully, the payment gateway confirms the customer has passed the identity authentication, sends the payment information, obtain the processing result from the bank, and forwards the processing result to the customer and the merchant.

[139] Wherein, the above authorization code is generated dynamically, and the generation rules can be adjusted by the payment gateway in real time. In the payment gateway, the rules themselves are variable dynamically and have certain validity periods. The authorization code can also be configured with a certain validity period as required. In this way, both the authorization code and the generation rules are variable dynamically, with validity periods; in addition, the authorization code is transmitted through a non-Internet approach, and the receiving terminal for the authorization code usually can't be obtained easily by others; therefore, security of online transactions can be ensured.

[140] According to an embodiment of the present invention, in the above system, the customer terminal that receives the authorization code can be specified; for example, a customer can register several records during registration of initial information in the payment gateway, and, during the transaction process, the customer can specify to send the authorization code to a specific customer terminal, so as to minimize the possibility of stealing the authorization code by others.

[141] After the customer browses the web pages provided by the merchant and submits a transaction request and the merchant receives

that transaction request, the online payment authentication method described in the invention will begin. Specifically, said method according to an embodiment of the present invention includes the following steps:

[142] The customer initiating a payment request on a web page provided by the merchant and entering into the interface of the payment gateway;

[143] The payment gateway requesting the customer to enter his/her online PIN and password for online payment over Internet for customer identity authentication and verifying said password;

[144] If the password for online payment is incorrect, the payment gateway rejecting the payment request; if the password for online payment is correct, the payment gateway generating an authorization code dynamically and it proceeding to the next step;

[145] The payment gateway sending the authorization code to the customer via the assistant customer identity authentication system;

[146] The customer entering the authorization code on the correct page in the payment gateway after he/she receives the authorization code;

[147] The payment gateway confirming the customer identity has passed the authentication after it verifies the authorization code successfully and then sending a payment request;

[148] Above payment request being sent to the bank's information processing system to complete the payment request.

[149] Said assistant customer identity authentication system forwards the authorization code to the customers through a non-Internet approach.

[150] After the payment gateway sends the payment request to the bank's information processing system, the bank's information processing system will execute payment operations and feed back the

result to the payment gateway.

[151] In the above steps, the online PIN is a code representing the customer identity for online payment, set by the customer in the payment gateway in advance; the password for online payment is a password set for authenticating the online PIN; generally spoken, the password shall be distinguished from the customer's account password, so as to enhance security.

[152] When a mobile telephone is used as the customer terminal and a SMS is used as the switch system for the assistant authentication system, the online payment authentication method according to an embodiment of the present invention includes the following steps:

[153] The customer sending a payment request on a web page provided by the merchant and entering into the interface of the payment gateway of the online payment system, choosing the assistant identity authentication as SMS-based authentication, and entering the mobile telephone number and the specified password for online payment at the prompt on the interface;

[154] When receiving the customer information, the payment gateway judging the mobile telephone number and the password for online payment; if said mobile telephone number has initial information registered in the payment gateway and the password is correct, the payment gateway generating an authorization code dynamically.

[155] The payment gateway sending said authorization code and the customer's mobile telephone number to the SMS center;

[156] The SMS center sending the received authorization code to the customer's mobile telephone;

[157] When receiving the short message, the customer entering the authorization code on the payment page at the prompt on the page;

[158] After verifying the authorization code successfully, the payment gateway deeming the customer's identity has passed the

authentication and it proceeding to the payment procedure.

[159] The authorization code is generated dynamically, with a validity period; the authorization code must be inputted within the specified validity period.

[160] The payment gateway sends said authorization code to the customer (i.e., the customer terminal) via the assistant customer identity authentication system; said customer terminal may be a customer terminal with its initial information registered in the payment gateway or a customer terminal chosen or specified by the customer. For example, a mobile telephone is usually chosen as the customer terminal for receiving the dynamic authorization code, whereas a BP or any other device can be used.

[161] In that way, during an online transaction, the mobile telephone number is used as the customer's PIN, as indicated in the registration of initial information, so that it is unnecessary to provide the customer's actual PIN or bank card ID over the network, and thereby the security is enhanced; in addition, the password-based authentication approach is flexible and convenient, and can meet the demands of the consumers.

[162] The information received by said switch system from said payment gateway can include authorization code and transaction information. Likewise, the information sent to the customer can include authorization code and transaction information. In addition, the short message containing the authorization code can be sent and received in the general encryption mode or re-encryption mode of the switch system.

[163] The switch system can use existing facilities, such as telecom networks and CATV networks, etc.

[164] In the above embodiment, the architecture of the online payment system provided in the invention is as follows: it involves two

physical platforms: one is a platform on Internet; the other is a telecom SMS platform.

[165] The system includes the following components: customer (i.e., card holder or buyer), online merchant, payment gateway, bank's information processing system, the payer's bank of account or agency bank,, SMS center, and short message receiving terminal - mobile telephone.

[166] Wherein, the customer, online merchant, payment gateway, bank's information processing system, the payer's bank of account and the payee's bank of account are connected over Internet; however, the customer and the merchant can only access or communicate with the payment gateway, but can't connect the bank's information processing system; the bank's information processing system is connected to the payment gateway, the payer's bank of account, and the payee's bank of account. The payment gateway sends payment requests to the bank's information processing system and obtains the processing result from that system; in this embodiment, the payment gateway is not connected directly to the bank.

[167] The customer terminal of said assistant customer identity authentication system can be a dedicated device separately configured or configured in any other electronic or electrical device such as a STB or a remote controller; or, the customer terminal of said assistant customer identity authentication system can be a non-dedicated device, such as a telephone, a mobile telephone, a BP, or a PDA; however, before the non-dedicated device is used as the customer terminal, it shall have its initial information registered in the payment gateway or a place specified by the payment gateway.

[168] In above assistant authentication system, a telecom SMS platform is used as the switch system, which authenticates the merchant with certificate and authenticates the customer in two times:

one is authentication with the password; the other is authentication with the dynamic authorization code.

[169] The service flow of the online payment system according to an embodiment of the invention can be as follows:

[170] Service flow 1

[171] The customer chooses merchandise at the merchant's website and creates an order, and submits a payment request;

[172] The customer enters into the payment page of the online payment system, chooses payment with mobile telephone; the page prompts the customer to enter the mobile telephone number and the password for online payment, and sends the mobile telephone number and the password for online payment to the payment gateway;

[173] When receiving the customer's information, the payment gateway judges the mobile telephone number and the password for online payment; if said mobile telephone number has initial information registered in the payment gateway, the payment gateway generates an authorization code that is unpredictable, and composes a short message containing the authorization code and the payment amount;

[174] The payment gateway sends the short message to the SMS center;

[175] The SMS center forwards the short message to the customer's mobile telephone;

[176] When receiving the short message, the customer verifies the payment amount and enters the authorization code on the payment page at the prompt on the page;

[177] The payment gateway verifies the authorization code, and then sends the information to the transaction processing system of the payer's bank of account after successful verification.

[178] The transaction processing system executes the deduction request, and then return the processing result to the payment

gateway;

[179] The payment gateway forwards the processing result to the merchant and the customer.

[180] Service flow 2

[181] The card holder chooses merchandise at the merchant's website and creates an order;

[182] When the customer chooses the payment mode as "payment with bank card + authentication with short message", the customer enters into the payment page of the online payment system, and enters the mobile telephone number and the password for online payment at the prompt on the page;

[183] When receiving the customer's information, the payment gateway judges the mobile telephone number and the password for online payment; if said mobile telephone has been costumed, the payment gateway generates an authorization code;

[184] The payment gateway sends said authorization code and the payment amount to the SMS center;

[185] The SMS center forwards the received authorization code and payment amount to the customer's mobile telephone;

[186] When receiving the short message, the customer verifies the payment amount and enters the mobile telephone number and authorization code on the payment page at the prompt on the page;

[187] The payment gateway verifies the authorization code, and then sends the deduction information to the bank's information processing system after successful verification;

[188] The bank's information processing system sends a deduction request to the payer's bank of account;

[189] The payer's bank of account deducts the amount from the customer's account, and returns the processing result to the bank's information processing system;

[190] The bank's information processing system returns the processing result to the payment gateway;

[191] The payment gateway records the transaction result and forwards the transaction result to the merchant; after receiving the notification for successful payment, the merchant provide the specified merchandise or service to the card holder.

[192] The above authentication method according to the embodiment of the present invention has the following advantages:

[193] The "mobile telephone short message" authentication mode for online payment effectively avoids illegal online transactions in case the card ID and the password are intercepted, and thereby effectively protects benefit of the cardholder. Since the card holder has to pass the two-stage authentication with password and authorization code contained in the mobile telephone short message, the identity authenticity of the cardholder can be ensured.

[194] In the "mobile telephone short message" authentication mode, the parties involved in online payment needn't to perform large-scale technical renovation or upgrade; as the result, from the viewpoint of economical efficiency, such an authentication mode is easy to use and low in cost.

[195] In the "mobile telephone short message" authentication mode for online payment, on one hand, the SSL encryption technique is still used in the technical plane; at the other hand, it eliminates the drawback of certificate-based authentication for the card holder, and eliminates the possibility that the card holder's confidential information is obtained by the merchant or even the acquirer.

[196] The present invention solves the problem regarding security in online payment: viewed from data security and integrity, the "short message" authentication mode employs effective encryption technique for data transmission and effectively isolates key

information in data stream from the merchant, and can prevent the key information from intercepted and illegally embezzled by network intruders;

[197] Viewed from authenticity of subjects involved in transaction, in the "mobile telephone short message" authentication mode, the card holder is authenticated twice, which is more secure than the simple password-based authentication in 3D Secure system.

[198] Since the customer needn't to enter credit card ID, ATM PIN, or validity period of credit card, the authenticate mode can eliminate the risk that the sensitive information is intercepted by hackers in network transmission.

[199] To make an online transaction, the customer must enter the mobile telephone number and the dedicated service password for online payment for preliminary identity authentication and then enter the unique dynamic authorization code for online payment dynamically received with the mobile telephone for secondary authentication; even if the preliminary authentication information is intercepted, the secondary authentication information can't be intercepted because the authorization code is generated by the online payment system uniquely and sent to the customer's mobile telephone through the SMS platform instead of the network; theoretically, the bi-channel security scheme employed in the authentication mode is more secure and harder to break when compared to mono-channel security schemes, and thereby can enhance security in online payment greatly.

[200] Such a password-based authentication mode is more flexible and easier to be accepted than the certificate-based authentication mode.

[201] Since mobile telephone has become a popular communication utility, the authentication mode is very convenient and the operating

procedures are simple and clear. The user will face a uniform payment interface during payment with different bank cards and needn't to understand different rules of the banks or master different operations. In addition, such an authentication mode can reduce the cost.

[202] Initial registration of customer information and activation/cancellation of online payment function:

[203] The customer can apply for activation of online payment function in the authentication mode described in the invention to the card issuing bank and specify the mobile telephone number to be bound to the bank card, and can cancel the online payment function in the same way. The system supports binding a mobile telephone number to multiple bank card IDs.

[204] The payer's bank of account will send the information for service activation/cancellation to the payment gateway of the online payment system in real time; the system will store the information as the basis for authentication, and send an acknowledge message to the card holder.

[205] The customer can specify the limit for each payment as well as the payment limit for each day.

[206] The customer can apply for service activation/cancellation at the payer's bank of account in any of the following ways:

[207] 1) The customer applies at the bank's counter;

[208] 2) The customer applies over Internet;

[209] 3) The customer applies with a dedicated device, such as POS.

[210] The customer has to specified an online PIN during the registration of initial information; said PIN may be a mobile telephone number, account ID, an ID provided by the payment gateway, or a code chosen by the customer. During the online transaction, the customer can specify the terminal the authentication code returns

to after he/she passes the password authentication.

[211] Above description is only provided to describe and facilitate understanding the technical scheme in the present invention better, but not to limit the implementation of the present invention. Those skilled in the art can easily make substitutions or modifications to the embodiments of the present invention, without departing from the spirit of the present invention; however, any of such substitutions or modifications shall fall into the scope of the present invention.